

REMARKS

I. INTRODUCTION

Claims 12, 16, 17, 21 and 22 have been canceled. The Specification and claims 1, 13 - 15, 18 and 19 have been amended. No new matter has been added. Thus, claims 1 - 11, 13 - 15 and 18 - 20 remain pending in the present application. In view of the following remarks, it is respectfully submitted that all of the presently pending claims are allowable.

II. THE 35 U.S.C. § 102(b) REJECTIONS SHOULD BE WITHDRAWN

Claims 2, 6 - 11, 13 - 15 and 19 - 20 stand rejected under 35 U.S.C. § 102(b) as anticipated by International Application Publication WO 98/12615 to Yokomoto et al. ("Yokomoto"). (See 5/2/07 Office Action, p. 2).

Yokomoto describes a system for encryption of touch screen input which includes a plurality of protective covers designed to protect user input from unauthorized viewing and access. The covers are connected together to form a single thick protective cover over the perimeter of a computer monitor. (See Yokomoto, p. 4, lines 7 - 15).

Claim 1 recites "*a controller receiving the identifier from the pad and transmitting the encrypted identifier to a verification device*" and "*a first link, communicatively coupling the controller and the encrypting circuit*" in combination with "*a second link, communicatively coupling the controller and the pad*" and "*a housing enclosing the encrypting circuit, wherein the encrypting circuit, the controller, the first link and the second link are each embedded within the housing.*" Thus, claim 1 clearly recites that the encrypting circuit, the controller, the first link and the second link are each physically embedded within the housing. That is, the embedding is not a conceptual embedding, but an actual, physical placement of the

components within a body of the housing.

In contrast, Yokomoto describes a plurality of covers that are complementarily shaped for attachment via screws to form a unitary cover for a computer screen. (See Yokomoto, p. 4, line 16 - p. 7, line 5; Fig. 1). Circuit elements are arranged on a circuit board located on the underside of one of the covers. (*Id.* at p. 7, lines 7 - 15). Yokomoto fails to describe or suggest a housing. The apparatus of Yokomoto is a cover that protects the computer screen, but does not actually house anything. Thus, it is respectfully submitted that Yokomoto fails to either disclose or suggest "a housing enclosing the encrypting circuit, wherein the encrypting circuit, the controller, the first link and the second link are each embedded within the housing," as recited in claim 1.

In addition, it is also respectfully submitted that Yokomoto does not teach or suggest a controller that transmits an encrypted identifier to a verification device. Yokomoto describes the circuit board as including a main processor that interfaces with the circuit board via a direct connection that delivers incoming scanning signals to the main processor. (*Id.* at p. 7, lines 13 - 25). Scanned data is then fed to a separate encryption processor via another direct electrical connection. Encrypted data is stored in a memory before being sent to a remote processor. (*Id.* at p. 11, line 10 - 18). The encrypted data is not transmitted to the remote processor directly by the main processor, but rather through the memory. Thus, it is respectfully submitted that Yokomoto fails to disclose or suggest "a controller receiving the identifier from the pad and transmitting the encrypted identifier to a verification device," as recited in claim 1.

Based on these reasons, it is respectfully submitted that claim 1 is allowable. Because claims 2, 6 - 11 and 13 - 15 depend from, and, therefore include the limitations of claim 1, it is respectfully submitted that these claims are also allowable.

Claim 19 recites the step of "placing . . . a controller" and "a first link communicatively coupling the controller and the encrypting circuit adjacent in an access-resistant

housing” in combination with “a second link communicatively coupling the controller and the pad, wherein the encrypting circuit, the controller, the first link and the second link are each embedded within the housing.” Claim 19 further recites the steps of “entering the identifier on the pad” and “receiving the identifier at the controller” in combination with “communicating the identifier from the controller to the encrypting circuit” and “encrypting the identifier by means of the encrypting circuit” and “sending the encrypted identifier to the controller after the step of encrypting.” Thus, it is respectfully submitted that claim 19 is allowable for the same reasons as discussed above with reference to claim 1. Because claim 20 depends from, and, therefore includes the limitations of claim 19, it is respectfully submitted that this claim is also allowable.

III. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN

Claims 3-5 and 18 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Yokomoto in view of European Patent No. 0809171 to de Jesus et al. (“de Jesus”). (See 5/2/07 Office Action, p. 3).

de Jesus describes a secured processor including a data encoding circuit which receives PIN data, encrypts the data and sends the encrypted data via a data line to an auxiliary processor for processing and eventual transmission to a central processor. (See de Jesus, col. 6, lines 49 - 55). The secured processor includes an actual polling circuit which samples keypad input and a false polling circuit which mimics actual sampling conducted by the actual polling circuit. (Id. at col. 5, line 42 - col. 6, line 9).

It is respectfully submitted that de Jesus fails to cure the deficiencies of Yokomoto. In particular, according to de Jesus, the secured processor performs encryption of PIN data. This encryption is controlled by an auxiliary processor, which instructs the secured processor to encrypt the PIN data before sending the encrypted data to the auxiliary processor. (See de Jesus, col. 14, lines 43 - 58). It is respectfully submitted that the secured processor is

not analogous to the controller recited in claim 1. As recited in claim 1, the controller transmits the identifier to the encrypting circuit. This is possible because, as recited in claim 1, the controller is coupled to the encrypting circuit via a first link. Thus, the secured processor of de Jesus cannot be analogous to both the controller and the encrypting circuit because the same device cannot be coupled via a link.

In addition, de Jesus describes the secured processor as being coupled to the keypad via a transmission line 3 and to the auxiliary processor via separate data lines 5 and 23. (*Id.* at col. 4, lines 17 - 24). According to de Jesus, the component which is directly coupled to the keypad (i.e., the secured processor) is also the encrypting component. It is only after the PIN data is encrypted that the encrypted data is sent to the auxiliary processor for forwarding to a central processor. (*Id.* at col. 6, lines 49 - 55). Thus, it is respectfully submitted that de Jesus neither discloses nor suggests "a controller receiving the identifier from the pad and transmitting the encrypted identifier to a verification device," as recited in claim 1.

In addition, de Jesus does not disclose or suggest embedding a second link between a controller and the encrypting circuit. de Jesus describes the secured processor as being mounted on a first circuit board substrate and encapsulated between two further circuit board substrates. (*Id.* at, col. 16, lines 32 - 52). Although the secured processor itself is encapsulated, no mention or suggestion is made that either the auxiliary processor or the links 5, 23 between the auxiliary processor and the secured processor are also encapsulated. Thus, it is respectfully submitted that de Jesus neither discloses nor suggests "a first link, communicatively coupling the controller and the encrypting circuit" and "a second link, communicatively coupling the controller and the pad" and "a housing enclosing the encrypting circuit, wherein the encrypting circuit, the controller, the first link and the second link are each embedded within the housing," as recited in claim 1.

Based on these reasons, it is respectfully submitted that neither Yokomoto nor de Jesus, either alone or in combination, discloses or suggests "*a controller receiving the identifier*

from the pad and transmitting the encrypted identifier to a verification device” and “a first link, communicatively coupling the controller and the encrypting circuit” in combination with “a second link, communicatively coupling the controller and the pad” and “a housing enclosing the encrypting circuit, wherein the encrypting circuit, the controller, the first link and the second link are each embedded within the housing,” as recited in claim 1. Because claims 3 - 5 depend from, and, therefore include the limitations of claim 1, it is respectfully submitted that these claims are allowable for the same reasons.

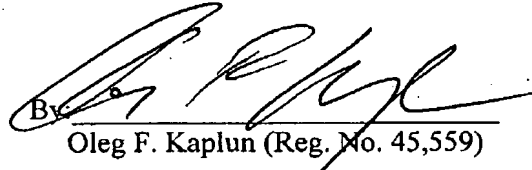
Claim 18 recites “a controller receiving the identifier from the pad and transmitting the encrypted identifier to a verification device” and “a first link, communicatively coupling the controller and the encrypting circuit” in combination with “a second link, communicatively coupling the controller and the pad” and “a housing, resistant to access and at least partially of chip on-glass technology, in which the first link, the second link and encrypting circuit are embedded.” Thus, it is respectfully submitted that claim 18 is allowable for the same reasons as claim 1.

IV. CONCLUSION

In light of the foregoing, Applicants respectfully submit that all of the now pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, and an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: June 20, 2007


By _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel: (212) 619-6000
Fax: (212) 619-0276/(212) 208-6819